CLAIMS

What is claimed is:

1. A method comprising:

receiving, at a server, a request from a client to take an action with respect to an electronic document;

obtaining, at the server and in response to the request, a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure; and

sending the authentication program to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document.

2. The method of claim 1, wherein obtaining the software program comprises requesting and receiving the software program from a second server.

3. The method of claim 1, further comprising:

receiving an updated authentication procedure;

receiving a subsequent request from the client to take the action with respect to the electronic document;

obtaining, in response to the subsequent request, a new software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting the updated authentication procedure; and

sending the new software program to the client for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document-permissions information associated with the electronic document.

4. The method of claim 1, wherein the software program uses an existing interface provided by the client to communicate authentication information to the server.

5. The method of claim 1, further comprising:

receiving credentials information from the client derived at least in part based on input obtained by the client using the software program; and

communicating with a third party authentication server to authenticate the current user based on the credentials information.

6. The method of claim 5, wherein the input obtained by the client comprises text input.

7. The method of claim 5, wherein the input obtained by the client comprises biometric data.

8. The method of claim 1, further comprising:

receiving from the client an authentication receipt obtained by the client from a third party authentication server based on input obtained by the client using the software program; and

verifying the current user with the third party authentication server using the authentication receipt.

9. The method of claim 1, further comprising:

retrieving a document identifier from the request;

determining whether user authentication is needed based on the document identifier and the action;

sending information specifying an acceptable authentication procedure; and

receiving an authentication procedure update request from the client.

10. The method of claim 1, wherein the document-permissions information specifies access permissions at a level of granularity smaller than the electronic document.

11. The method of claim 10, wherein the level of granularity comprises a per-page granularity for the specified access permissions.

12. A software product tangibly embodied in a machine-readable medium, the software product comprising instructions operable to cause one or more data processing apparatus to perform operations comprising:

receiving a request from a client to take an action with respect to an electronic document;

obtaining, in response to the request, an authentication process; and

sending the authentication process to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document.

13. The software product of claim 12, wherein obtaining the authentication process comprises requesting and receiving the authentication process from a second server.

14. The software product of claim 12, wherein the operations further comprise:

receiving a subsequent request from the client to take the action with respect to the electronic document;

obtaining, in response to the subsequent request, a new authentication process; and

sending the new authentication process to the client for use in identifying the current user and controlling the action with respect to the electronic document based on the current user and the document-permissions information associated with the electronic document.

15. The software product of claim 12, wherein the authentication process uses an existing interface provided by the client to communicate authentication information to the server.

16. The software product of claim 12, wherein the operations further comprise:

receiving credentials information from the client derived at least in part based on input obtained by the client using the software program; and

communicating with a third party authentication server to authenticate the current user based on the credentials information.

17. The software product of claim 16, wherein the input obtained by the client comprises text input.

18. The software product of claim 16, wherein the input obtained by the client comprises biometric data.

19. The software product of claim 12, wherein the operations further comprise:

receiving from the client an authentication receipt obtained by the client from a third party authentication server based on input obtained by the client using the software program; and

verifying the current user with the third party authentication server using the authentication receipt.

20. The software product of claim 12, wherein the operations further comprise:

retrieving a document identifier from the request;

determining whether user authentication is needed based on the document identifier and the action;

sending information specifying an acceptable authentication procedure; and

receiving an authentication procedure update request from the client.

21. The software product of claim 12, wherein the document-permissions information specifies access permissions at a level of granularity smaller than the electronic document.

22. The software product of claim 21, wherein the level of granularity comprises a per-page granularity for the specified access permissions.

23. A system comprising:

a client that sends a request to a server when an action is to be taken with respect to an electronic document local to the client;

the server that receives the request, and in response to the client, the server obtains and sends a software program comprising instructions operable to cause one or more data processing apparatus to perform operations effecting an authentication procedure; and

wherein the client uses the authentication program to identify a current user and control the action with respect to the electronic document based on the current user and document-permissions information associated with the electronic document.

24. The system of claim 23, further comprises a second server that provides the software program.

25. The system of claim 23, wherein the client includes a security handler that provides a server-communication interface to the software program.

26. The system of claim 23, further comprising a third party authentication server that authenticates the current user based on credentials information derived at least in part based on input obtained at the client using the software program.

27. The system of claim 26,wherein the client obtains an authentication receipt from the third party authentication server and forwards the authentication receipt to a server for verification.

28. The system of claim 23, wherein the server comprises:

a server core with configuration and logging components;

an internal services component that provides functionality across dynamically loaded methods; and

dynamically loaded external service providers, including an authentication service provider.

29. The system of claim 23, further comprising:

a business logic tier comprising a cluster of document control servers, including the server;

an application tier including the client comprising a viewer client, a securing client, and an administration client; and

a load balancer that routes client requests to the document control servers.

30. The system of claim 23, wherein the server comprises a permissions-broker server including a translation component, the local electronic document comprises a document secured previously by the permissions-broker server, and the translation component being operable to translate first document-permissions information in a first permissions-definition format into second document-permissions information in a second permissions-definition format in response to the request being received from the client.

31. The system of claim 23, wherein the server comprises a permissions-broker server operable to identify information associated with the local electronic document in response to the request, the associated information being retained at the server and indicating a second electronic document different from and associated with the local electronic document, the server being operable to relate information concerning the second electronic document to the client to facilitate the action to be taken.

32. The system of claim 23, wherein the server comprises a document control server operable to synchronize offline access information with the client in response to the client request, the offline access information comprising a first key associated with a group, the first key being useable at the client to access a distributed document by decrypting a second key in the distributed document, and the client allows access to the distributed document, when offline, by a user as a member of the group, using the first key to decrypt the second key in the distributed document and governing actions with respect to the distributed document based on document-permissions information associated with the distributed document.

33. A system comprising:

server means for dynamically obtaining and sending authentication processes in response to client requests to take actions with respect to electronic documents; and

client means for interfacing with a received authentication process to identify a current user and for controlling actions with respect to electronic documents based on the current user and document-permissions information.

34. The system of claim 33, further comprising:

server means for transparently providing offline access information for controlled documents to pre-authorize a client to allow actions by a user as a member of a group of users, the offline access information comprising a first key associated with the group, the first key being useable at the client to access an electronic document by decrypting a second key in the electronic document; and

client means for accessing the electronic document using the offline access information.